Have you ever considered a career in computer security but didn’t know how to get started?

The Information Security industry is an exciting and diverse place to work in the 21st century, but how do you get started, especially if you’ve no background in security? It seems that most advertised jobs (in newspapers, LinkedIn, Jobserve, etc.) require years of experience, and often ask for qualifications that are impossible to obtain for people new to the industry (such as the all-pervasive CISSP). What can you do to get your foot on the first rung of this very tall ladder and eventually land the job of your dreams?

What was once seen as a back-room career for hackers, geeks and mathematicians has completely changed over the last 10 years, evolving into an industry of many diverse and fascinating disciplines, from architects to business leaders, programmers to crypto engineers, and all the myriad jobs in between – here are a few of the job titles you might end up with if you obtain the right levels of experience and training:

- Information Security Manager
- Chief Security Officer
- Risk Manager
- Operational Security Manager
- Digital Forensics Analyst
- Security Architect
- Penetration Tester
- Security Requirements Manager
- Security Programmer
- Malware Analyst
- Intrusion Analyst
- Incident Response Manager
Or you might decide to become a Subject Matter Expert (SME) in some kind of security technology, such as:

- Firewalls
- Intrusion Prevention Systems
- Access Control Systems
- Smart cards
- Biometrics
- Encryption technology

This is not by any means an exhaustive list, instead it is used simply to illustrate the range of jobs, from technical to business roles, available in the security industry. Looking at this list it’s easy to see that there is something for most people should they wish to get involved. But how do you get started?

There are in fact many routes into the information security industry, some of which are easier to take than others. To reach the lofty heights of managing a professional hacking team (known in the industry as pen testing), for example, you will need many years of experience in working with customers, scoping penetration tests and ensuring that what you are doing yields the right level of results for your clients without creating an unrecoverable denial of service against their systems. Nevertheless, you could potentially get hired as a junior pen tester if you demonstrate the right mindset to your potential employer. Working as a systems administrator, for example, is a great place to start. If you are already in the IT industry in another area, you will more than likely be aware of what information security is all about. Taking the skills of a system admin forward into the security marketplace is not that hard. A really good system administrator who understands scripting and operating systems basics, who demonstrates an aptitude for finding and solving tricky problems, makes the best sort of penetration tester. Starting with a testing scope, such as to break into a particular application, the system administrator would use all the tools and techniques he’d normally use for finding why an application was misbehaving to locate weaknesses (known as vulnerabilities). Then, using some additional skills (which can be trained), the sys admin can then make the application misbehave and potentially give up some secrets. This is how hackers operate and how ethical hackers (working for good – and usually money) also operate.
What if you are a code monkey? There are plenty of programmers in the world who know very little about secure coding, so by learning the techniques and weaknesses of modern programming languages and system architectures, you can build code that is stronger and more resistant to hacking, and for this you can command a decent pay rise. Again, these are all skills that can be learned through academic and professional training.

So, it might seem that if you take a course in security coding, you can become a security professional? Is that true? Unfortunately not! To become a true security professional, using the most modern of definitions, you need a firm grounding right across many different aspects of security, not just your chosen specialised subject. This is why the organisation responsible for the baseline security qualification known as CISSP (Certified Information Systems Security Professional), (ISC)², has created a curriculum of study that is so wide and diverse. To become a Certified Information Systems Security Professional you need to pass a six hour exam covering ten separate business domains, as follows:

- Access Control
- Telecommunications and Network Security
- Information Security Governance and Risk Management
- Software Development Security
- Cryptography
- Security Architecture and Design
- Operations Security
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations and Compliance
- Physical (Environmental) Security

However, to get certified as a CISSP, you also need to demonstrate that you have 5 years operating at a professional level therefore, this is unobtainable for newbies just entering the industry. The problem is, no CISSP means no job in many cases, as the CISSP has become the HR gate you need to get through to even get as far as the interview stage. In an industry that is so unbelievably short of blood, it seems ridiculous that there is no way to get your foot on the ladder. There must be a better way. Well, there is now...
It was estimated earlier in 2014 that there are 2.2 million people employed in the global information security sector. By 2015, (ISC)2 predicts this number will have risen to 4.25 million security professionals. Yet, this is predicated on there being enough new blood coming into the industry to meet that growth target. The issue the industry faces is: how do we attract this new talent, especially into the niches within the niche, such as getting people into digital forensics, reverse engineering malware and penetration testing. One way to address this is, over the past few years, the UK and American governments have been running annual cyber security competitions to attract new talent into the industry. This competition in the UK is known as the “Cyber Security Challenge” and offers a series of information security-related competitions that anyone can have a go at. The trials get harder and harder until the final showdown between the last contestants eventually leads to a Cyber Security champion being crowned. Along with many of the other finalists, this Cyber Security champion receives all sorts of specialist training, job offers and academic scholarships.

Australia has followed suit with its own cyber security competition, which began in April 2012, and was hailed a great success by the media. These competitions serve an important purpose in identifying people with aptitude, raising awareness about the industry to the general public, and in most cases they generate many hours of media coverage (even inspiring full-length documentaries on information security). All this publicity helps expose the information security sector to those who might be interested but have not considered it as a viable option. Some statistics from Microsoft UK suggest the IT industry will generate 78,000 new jobs over the next four years, yet e-Skills UK has reported that its own research confirms a 50% decline in young UK residents entering the IT industry over the past five years. As only a small proportion of these new IT entrants make it into security, then there is an imminent crisis looming.

This is why the British Computer Society (BCS) has now developed its new professional Certificate in Information Security Management Principles. This course, unlike the CISSP, is an entry-level course and is open to anyone who is interested in getting into security. You can take a CISMP 5-day training course and at the end of it you are ready to take the exam, which is run by BCS. This exam covers all the same subject matter as the CISSP exam, but it doesn’t quite go as deep into the ten domains. Nevertheless, passing the CISMP is seen by the UK government as a good enough foundation to apply to become a CESG Listed Advisors Scheme consultant, which is the minimum requirement for government security professionals, therefore it’s rapidly becoming the must-have qualification to gain in Information Security.

InfoSec Skills provides an online version of the 5-day training course, therefore making it uniquely accessible for those people wanting to study to become security professionals, while still working in their day job.
The Certificate in Information Security Management Principles (CISMP) course is designed to provide the foundation of knowledge necessary for individuals who have information security responsibilities as part of their day-to-day role, or who are thinking of moving into an information security function.

The CISMP course and associated qualification provides the opportunity for those already serving as information security professionals to enhance or refresh their knowledge and, in the process, gain a recognised industry qualification, regulated by the British Computer Society (BCS). This is useful to both the individual and employer in terms of attesting to the level of professional ability an individual has attained.

CISMP covers the following areas:

- Information Security Management Principles
- Information Risk
- Information Security Framework
- Procedural/People Security Controls
- Technical Security Controls
- Software Development and Lifecycle
- Physical and Environmental Control
- Disaster Recovery and Business Continuity Management
- Other technical aspects
- Preparation for the CISMP Examination and Mock Exam

So, getting your foot in the door, with a professional qualification is the best start to a new career path. Whatever your current job, be it project manager, risk manager, programmer, systems administrator, or even if you are in an unrelated job, such as a property manager or a retail worker, there is a place for you in the security industry if you are interested in learning about it. Taking the CISMP is the best way to get started and it’s something that InfoSec Skills can help you with.
What's more, to really kick start your new career in Information Security and help you get recognised as a professional, when you pass the CISMP exam after training with InfoSec Skills, you are entitled to a free one year membership as an Associate Member of the British Computer Society (AMBCS), which gives you all the benefits of professional registration as well as a cool post-nominal to put after your name. Read on for more information...

**Associate Membership for successful BCS Professional Certification candidates**

We are providing successful BCS Professional Certification candidates with a year’s Associate (AMBCS) membership.

Access to membership for a year offers successful candidates a taste of what it’s like to belong to the leading industry body for IT and the kind of support they could receive to help them reach their career potential.

**Why become a member?**

‘I think that if you want to be considered a professional, it’s important to join your professional body. The Institute helps me keep abreast with current developments in the field and has added interest and satisfaction not only professionally but socially as well.’

Dr C James Bacon, MBCS

**How do Professional Certification candidates receive their membership?**

Following the successful completion of a BCS Professional Certificate and the notification of result, candidates will receive an activation email / letter with details of a dedicated web portal where they can complete their details and confirm their agreement to the BCS Code of Conduct.

This will activate their membership and they will then be able to start enjoying the full Associate (AMBCS) membership benefits package.

**The benefits of Associate (AMBCS) membership**

Associate membership delivers a range of services designed around the professional needs of today’s competent IT practitioners.

- **Professional recognition**
  Tools to gain recognition within the industry include post nominal letters AMBCS, and a defined path to Chartered status via Professional membership.

- **Career development**
  To plan and track progression, members use our CPD portal and full access to Browse SFIAplus, the online tool that allows them to explore the industry framework for IT skills, training and development.

- **Networking**
  Top people, great ideas and the latest thinking locally, nationally and online - our global networking opportunities are unrivalled and include branches, specialist groups and the Member Network.

- **Knowledge and best practice**
  From the latest industry news to our massive online library, the Institute’s information services keep members up to date with best practice, and at the cutting edge of IT.

- **Exclusive discounts and offers**
  Adding even more value to membership, our discounts and free services enable members to enjoy savings both at work and at home.
UK - Information Security Career Paths

This career path diagram illustrates the potential career progression you can make in information security. It recognises the importance of awarding body professional certificates and your experience over time, and provides a high level alignment with BCS membership grades, because these frameworks have either 3, 6 or 7 levels. This view allows you to map certificates to job roles and see what development needs should be followed to advance in seniority and even transition to a new career. Above all, we want to point you in the right direction and provide you with the links for further research so you can make an informed decision regarding your future.

### Personal Development

- Business management experience
- Strategic planning
- BCS: Fellow (FBCS) membership
  - Preparation for significant information security management role
- BCS: Chartered (CITP) IT Professional
  - Further practitioner courses and industry certifications
  - Seek higher level security roles and prepare to:
    - Take full organisational responsibility
    - Operate with higher level stakeholders
- Further practitioner courses and industry certifications to gain breadth and depth
  - Seek higher level security roles and prepare to:
    - Seek full organisational responsibility
    - Operate with higher level stakeholders
- IISP/BCS/APMG:
  - Further practitioner courses and industry certifications
  - Seek higher level security roles and prepare to:
    - Seek full organisational responsibility
    - Operate with higher level stakeholders

### Sample Professional Certificates

- CREST: Certified Web Application Tester (CCWAT)
- CREST Certified Infrastructure Tester (CCIT)
- CREST Certified Simulated Attack Specialist (CCASS)
- CREST Certified Threat Intelligence Manager (CCTIM)
- CREST Certified Wireless Specialist (CCWS)
- CREST Certified Network Intrusion Analyst (CCNA)
- CREST Certified Host Intrusion Analyst (CCHA)
- CREST Certified Malware Reverse Engineer (CCMRE)
- CREST Certified Incident Manager (CCIM)
- CREST Registered Threat Intelligence Analyst (CRIIA)
- CREST Practitioner Threat Intelligence Analyst (CPIA)
- CREST Registered Technical Security Architect (CTRSA)
- CREST Practitioner/Technical Security Architect (CTSP)
- CREST Registered Intrusion Analyst (CRIA)
- CREST Practitioner Intrusion Analyst (CPA)
- CREST Registered Penetration Tester (CRT)
- CREST Practitioner Security Analyst (CPSA)

### Professional

- ISACA:
  - CGEIT - Certified in the Governance of Enterprise IT
  - CISM - Certified Information Security Manager

- PCI DSS:
  - PCI DSS - Payment Card Industry Data Security Standard

- SANS:
  - GSEC - Security Essentials

- CompTIA:
  - CompTIA - Network+
  - CompTIA - Security+

### Further Reading

- BCS: Student membership
- BCS: Associate membership
- BCS: Chartered (CITP) IT Professional
- BCS: Fellow (FBCS) membership
- IISP/BCS/APMG:
  - Further practitioner courses and industry certifications
  - Seek higher level security roles and prepare to:
    - Seek full organisational responsibility
    - Operate with higher level stakeholders

### InfoSec Career Startpoint

- IT Technician
  - IT Customer Support

- Network Administrator
  - System Administrator
  - Network Engineer
  - Web Administrator
  - IT Technician
  - IT Technical Support

- Level 1 - Apprenticeship in Information Security

- Level 2 - Higher Apprenticeship in Information Security

- Level 3 - Advanced Apprenticeship in Information Security

- Level 4 - Higher Apprenticeship in Information Security